External Certification Authorities (ECAs)

Barbara Keller

DISA

November 20, 2003

ECA Requirement

"Secure interoperability between DoD and its vendors and contractors will be accomplished using External Certificate Authorities (ECAs). ECAs will operate under a process that delivers the level of assurance that is required to meet business and legal requirements….Requirements for interoperable PKI-enabled services with Industry partners shall be met via certificates generated from an IECA or ECA."

[DoD PKI Memo, 12 August 2000]

"To ensure secure interoperability between DoD and its vendors and contractors, interoperability will be accomplished in the near term using External Certification Authorities (ECAs)."

[DoD Target PKI ORD, 20 August 2001]

"Components may … modify or adjust their implementation dates as required, but in no case beyond April 2004."

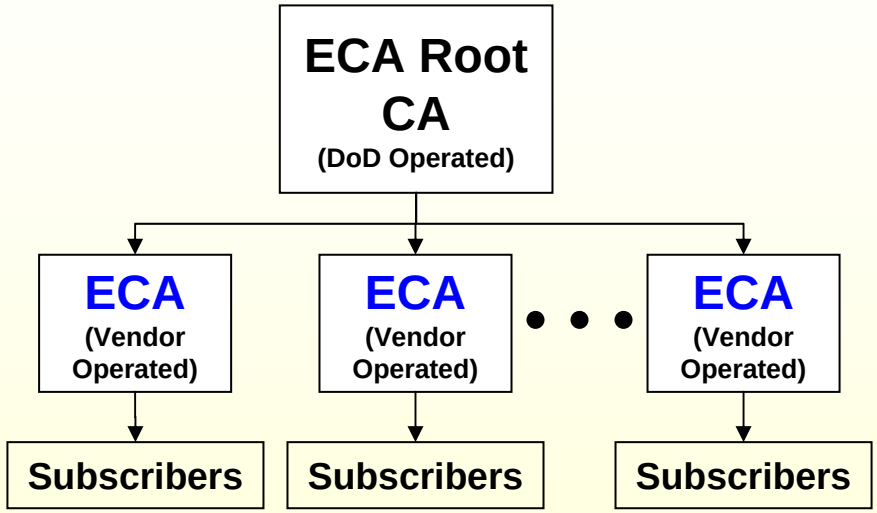
"The change in deadline for issuing CACs should not be considered a reason to slow PKI Implementation efforts, …"

[PKI and PKE Implementation Update, 7 October 2003]

ECA Background

- **Promote "Single Certificate" for Industry Partners across U.S. Government**
  - **Eliminate "DoD Only" usage requirement**
  - **Permit marketing and use of ECA certificates to support Federal, State, and Local Government needs**
- **Comply with DoD X.509 Certificate Policy**
- **Implement Cost-effective Solution for Industry Partners and DoD**
  - **Continue to seek and incorporate industry comments on functionality and assurance level**
- **Reduce or Eliminate GOTS requirements**

ECA Architecture



- **ECAs are operated by commercial vendors**
  - **Certificate fees are permitted**
  - **Certificate Revocation List (CRL) data available at no charge.**
- **The ECA Root CA will issue subordinate CA certificates to ECA vendors**
- **ECAs operate under MOAs and certificate and key recovery policies**

ECA Key Points

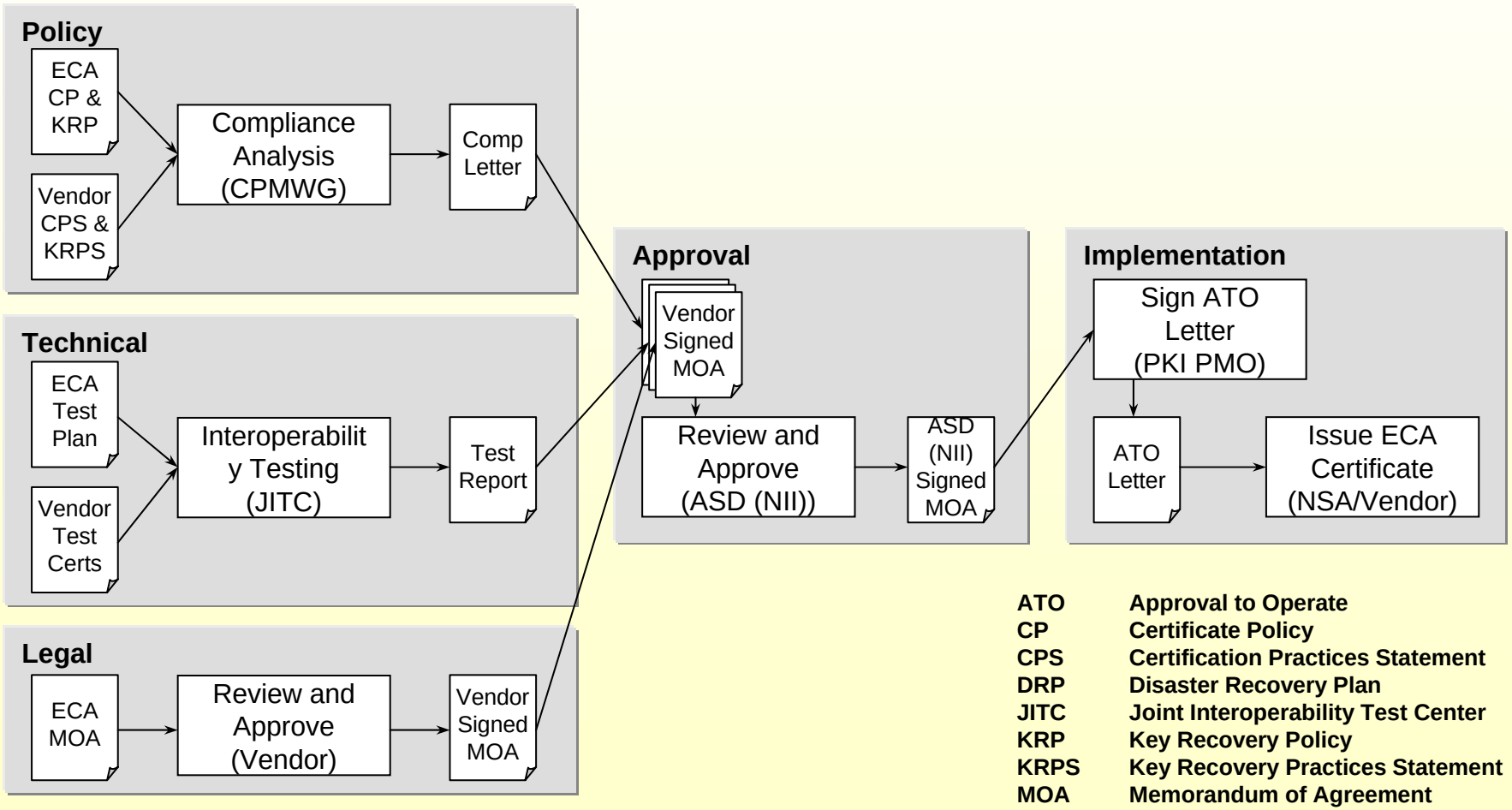
- **Certificate Management**
  - Puts the responsibility on the subscriber's sponsoring organization (generally their company) for keeping certificate information current
  - Registration infrastructure is provided by ECAs
- **Liability**
  - Cleanly separates DoD PKI from the ECA PKI
  - Explicitly removes liability from the DoD and the US Government for improper issuance and use of ECA certificates
  - ECAs must accept liability for improper operation but may limit liability to $1,000 per transaction and $1,000,000 per incident
- **Assurance Level**
  - Ensures that certificates issued under the ECA program meet minimum DoD requirements

Status of ECA Program

- ✓ ECA Certificate Policy and Key Recovery Policy Signed by the Hon. Mr. Stenbit, June 2003
- ✓ ECA Root Certification Authority Certification Practice Statement signed by Mr. Nolte, June 2003
- ✓ ECA Root Certification Authority established, June 2003
- ✓ ECA Interoperability Test Plan completed, September 2003
- ✓ ECA Memorandum of Agreement draft text approved, October 2003
- ✓ ECA Root CA testing completed, October 2003

Transition to ECA

Transition Approach



ATO	**Approval to Operate**
CP	**Certificate Policy**
CPS	**Certification Practices Statement**
DRP	**Disaster Recovery Plan**
JITC	**Joint Interoperability Test Center**
KRP	**Key Recovery Policy**
KRPS	**Key Recovery Practices Statement**
MOA	**Memorandum of Agreement**

Enabling Applications to Accept ECA Certificates

- **Testing the application**
  - **ECAs will not support test certificates - instead, ECA certificates have been fully tested prior to granting ECA status**
  - **Use test certificates from the DoD test PKI for application testing**
- **Architect and implement a process for granting access to external certificate holders**
  - **For example: Require that holders self-register to the directory, then have their DoD sponsor send a digitally signed email requesting that access be granted, then manually add subscriber to the appropriate access group**
- **Implement a mechanism for accessing ECA CRLs**
  - **Determine CRL access points from the ECA web site**
  - **If using OCSP, ensure that the OCSP responder is processing ECA CRLs**

Enabling Applications to Accept ECA Certificates (cont.)

- **Add the ECA Root CA to the application trust list**
  - **IECA CA Certificates and CRLs can be accessed from the ECA web site:**
    - **http://iase.disa.mil/pki/eca**
  - **In the future, ECA CA Certificates and CRLs will be posted to the Global Directory Service, and ECA CA Certificates will be included in the installroot tool**
  - **The ECA root will be submitted for membership in the Federal Bridge**
- **Provide guidance to help desk staff for addressing user requirements from IECA/ECA subscribers**


DEFENSE INFORMATION SYSTEMS AGENCY